动态分组混沌伪随机数发生器 *

曹艳艳 [1,2]，杨　波 [1,2†]

(1. 陕西师范大学 计算机科学学院，西安 710119；2. 中国科学院信息工程研究所，信息安全国家重点实验室，北京 100093)

摘　要：为了克服计算机处理数据的有限精度导致混沌特性退化的缺陷，改善随机数发生器输出序列的随机性能，设计了一种新的基于 Logistic 混沌映射生成伪随机数的方法。在提出的方法中，采用四个一维 Logistic 混沌映射，每次迭代随机选择扰动源对其他三个 Logistic 映射进行扰动，加入可变扰动参数，组合时随机动态分组，从而提高序列的随机性能，扩大序列周期，避免序列的重复出现。以新方法设计的伪随机数发生器易于软件实现，生成的序列通过随机数检测标准 NIST SP800-22，从而具有良好的随机性，可用于保密通信等信息安全领域。

关键词：混沌系统；Logistic 映射；伪随机数发生器；S-box

中图分类号：TP309.2　　doi: 10.3969/j.issn.1001-3695.2018.02.0103

Chaotic pseudorandom generators based on dynamically group

Cao Yanyan[1, 2], Yang Bo[1, 2†]

(1. *School of Computer Science Shaanxi Normal University*, *Xi'an* 710119, *China*; 2. *State Key Laboratory of Information Security*, *Institute of Information Engineering*, *Chinese Academy of Sciences*, *Beijing* 100093, *China*)

Abstract: In order to overcome the degration of chaotic and improve the randomness of the sequence, this paper proposed a new method of generating pseudo-random numbers based on Logistic chaotic mapping . It used four one-dimensional Logistic chaotic maps. Each iteration randomly selected one to perturb the other three Logistic maps, adding variable parameters and randomly grouping them dynamically to improve the randomness of the sequences. Meanwhile, it enlarged the period of sequence and avoided recurrence of sequences . The pseudo-random number generator is easy to implement by software. The sequence can pass the NIST SP800-22 randomness test. It has good randomness and can apply in the field of information security such as secure communication.

Key words: chaotic system; logistic map; pseudorandom generator; S-box

0　引言

随机数广泛应用于加密及签名等，其随机性能影响加密及签名方案的安全，因此研究构造性能良好的随机数发生器已成为必然趋势。随机数发生器主要分为真随机数发生器和伪随机数发生器。真随机数发生器一般采用物理方法生成，主要包括直接放大法、振荡采样法和亚稳态采样法。首先，真随机数发生器需要随机性很高的物理熵源，而物理熵源易受到外部环境的影响，从而影响序列的随机性能。其次，真随机数发生器需要的成本高。为了克服真随机数发生器以上缺点，学者们继而研究了伪随机数发生器。伪随机数发生器是确定性算法。输入种子，经过多次迭代，获得与真随机数序列接近的伪随机数序列。

混沌是确定但不可预测的复杂动力学现象。混沌映射对初始值敏感而表现出的不可预测、类似随机性的特性广泛应用于伪随机数发生器的构造。利用混沌构造伪随机数发生器易于软件实现，生成速率较快。Lorenz[1]于 1963 年发现混沌现象。随后，混沌在安全通信[2]、文本加密[3]以及生成随机数[4~14]等方面，取得了良好的效果。Wang 等人[4]利用基于分段 Logistic 映射，García-Martínez 等人[5]利用 k-modal 映射和 Murillo-Escobar 等人[6]利用提高的 Logistic 映射构造伪随机数发生器。利用这些改进 Logistic 映射构造的伪随机数发生器，改善生成序列的随机性能，但是其计算量较大。Patidar、François 和 Tamilselvi 等人[7~10]相继提出多个 Logistic 映射组合的方式，进一步改善了

收稿日期：2018-02-01；**修回日期：**2018-03-20　**基金项目：**国家重点研发计划资助项目（2017YFB0802000）；国家自然科学基金资助项目（61572303，61772326）；国家“十三五”密码发展基金资助项目（MMJJ20170216）；中国科学院信息工程研究所信息安全国家重点实验室开放课题（2017-MS-03）；中央高校基本科研业务费项目（GK201702004）

作者简介：曹艳艳（1993-），女，河北保定人，硕士研究生，主要研究方向为密码学；杨波（1963-），男（通信作者），陕西富平人，教授，主要研究方向为公钥密码学等（by@snnu.edu.cn）．

序列的随机性能，但是在数字化过程中，未能克服混沌退化对序列随机性的影响。Liu 等人[11]利用 Chen 连续超混沌系统和董丽华等人[12]利用六维细胞神经网络构造伪随机数发生器，通过增加计算成本，提高输出序列的随机性能。Bahi 等人[13]提出扰动优化和 Wang 等人[14]将混沌与可变扰动参数相结合构造的伪随机数发生器，扩大随机序列的周期。为了克服有限精度导致混沌退化，提高生成序列的随机性能，本文利用动态分组的随机数生成方法。该方法采用四个一维 Logistic 映射生成伪随机序列。每次迭代随机选择一个 Logistic 映射作为扰动源对其他三个Logistic映射进行扰动，随后生成的数据经过S盒[15]变化，动态分组，每次生成 16 位伪随机序列。参数进行动态更新，从而有效避免序列重复出现，扩大序列的周期。测试结果表明该方法生成的随机序列符合国际随机数检测标准 NIST SP800-22 的要求。

1　相关混沌映射

Logistic[16]混沌映射是一维非线性离散混沌系统，因其实现简单，计算量少，经常用于图像加密及伪随机数的生成。其迭代方程为

$$x_{n+1} = \mu x_n(1-x_n)\text{。}$$

其中：x_n 为迭代状态值，取值范围为 $(0,1)$；μ 为控制参数。图 1 为 Logistic 的倍周期分叉图，横轴表示控制参数，纵轴表示迭代状态值。当 μ 不断变化时，其迭代过程发生显著的变化。$\mu > 3.57$，Logistic 映射进入混沌状态。为了提高序列随机性能，Logistic 映射的控制参数取值为：3.9999。

Lyapunov 指数刻画混沌系统对初始值的敏感性。给定两个相差微小的初始值，系统会随着时间变化产生两种截然不同的运动轨迹。当 Lyapunov 指数是负数时，表明该系统的运动轨迹是收缩的，在相应方向上的状态趋于稳定；反之，当 Lyapunov 指数是正数时，表明系统进入混沌状态，不可预测其运动轨迹。混沌初始值分别为 0.000125，0.0001251，迭代 100 次后的轨迹如图 2 所示。

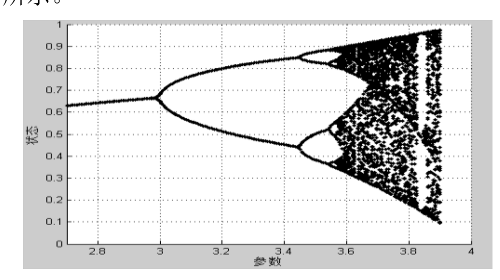


图 1 Logistic 映射的倍周期分叉图

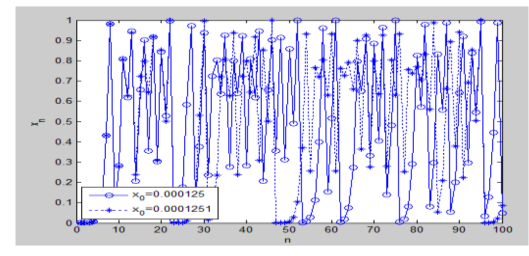


图 2　不同初值的轨迹图

图 2 表明随着混沌迭代次数的增加，相差十分微小的两个初始值产生两种截然不同的轨迹，这一特性很难确定混沌的初始值，从而保证了混沌用于加密时的安全性。

2　伪随机数生成方法

随机数生成方法具体由以下步骤组成（$S(x)$ 表示 AES 加密的 S 盒变化）：

a)初始化。密钥流序列 K：

$$K = k_{1-16}k_{17-32}k_{33-48}k_{49-64}k_{65-72}k_{73-80}k_{81-88}k_{89-96}$$
$$k_{97-104}k_{105-112}k_{113-120}k_{121-128}k_{129-136}k_{137-144}k_{145-152}$$

密钥流序列 $K_1(k_{1-16})$，$K_2(k_{17-32})$，$K_3(k_{33-48})$，$K_4(k_{49-64})$ 初始化四个 Logistic 的初始值 x_1，x_2，x_3，x_4，每个密钥 16 bits，共 64 bits；$K_5(k_{65-72})$，$K_6(k_{73-80})$，$K_7(k_{81-88})$，$K_8(k_{89-96})$，$K_9(k_{97-104})$，$K_{10}(k_{105-112})$，$K_{11}(k_{113-120})$，$K_{12}(k_{121-128})$，$K_{13}(k_{129-136})$，$K_{14}(k_{137-144})$，$K_{15}(k_{145-152})$ 初始化参数 C_1，C_2，C_3，C_4，C_5，C_6，C_7，C_8，C_9，C_{10}，C_{11}，每个参数 8 bits，共 88 bits。

b）每个 Logistic 迭代 100 次，进入混沌状态。

c）根据随机扰动参数 C_1 选择扰动顺序：

$$i = C_1 \bmod 4$$

第 i 个 Logistic 映射做为扰动源，对其他的 Logistic 映射进行随机扰动:

$$x_{(i+1)\bmod 4} = x_i + x_{(i+1)\bmod 4}$$
$$x_{(i+2)\bmod 4} = x_i / 2 + x_{(i+2)\bmod 4}$$
$$x_{(i+3)\bmod 4} = x_i / 4 + x_{(i+3)\bmod 4}$$

四个 Logistic 映射输出数据根据 $(C_2 \bmod 4)$ 奇偶性（C_3，C_4，C_5 相同处理）进行左移或右移（偶数左移，奇数右移）。每个数据移位处理后的四个数据经过 S 盒变化后形成 4*4 的矩阵。

d）主对角线、副对角线分别将矩阵分成了两个区域。当参数 C_6 为偶数时，输出的两个数据 P_1, P_2 是主对角线划分的两个区域数据的异或和。当参数 C_6 为奇数时，输出的两个数据 P_1, P_2 是副对角线划分的两个区域数据的异或和。

e）扰动参数 Q 是由密钥 $(C_7C_8C_9C_{10})$ 控制的可变参数经过 S 盒变化后的数据，其中 Q 如下：

$$Q = S(C_7C_8^3 + C_9C_{10}^2)$$

f）最后输出的伪随机数分别为

$$P_1' = S(P_1 \oplus Q)\text{，}\quad P_2' = S(P_2 \oplus Q)$$

g）根据 $(C_{11} \bmod 4)$ 奇偶性进行拼接，拼接方式如下：若为奇数输出的伪随机序列：$P = P_1' \| P_2'$，否则 $P = P_2' \| P_1'$

h）参数 $(C_1C_2C_3C_4C_5C_6C_7C_8C_9C_{10}C_{11})$ 更新，参数 $(C_2C_3C_4C_5C_8C_9)$ 与 P 的前 8 位进行异或操作。其他参数与 P 的后 8 位进行异或操作。

i）重复 c)~h)多次，直到输出指定长度的序列为止。

3　安全性分析

3.1　密钥空间分析

为使随机数发生器拥有足够大的密钥空间来抵抗穷举攻击，本文采用四个 Logistic 混沌映射交替扰动，多参数参与运算，动态分组的构造方法。每个 Logistic 映射采用 16 位密钥进行初始值设置，十一个参数分别用 8 位密钥进行初始值设置。与文献[5,6]进行密钥长度比较，结果如表 1。本方案密钥长一共有 152 位，大于 128 位，可有效的抵抗穷举攻击。

表 1　密钥长度分析表

方法	密钥长度
文献[5]	159
文献[6]	128
本文方法	152

3.2　密钥敏感性分析

利用混沌构造伪随机数发生器，应该保持混沌对初值敏感性的特性。位变化率[17]衡量混沌伪随机数发生器对初值敏感性的程度。位变化率即对密钥仅做微小改变后，生成的伪随机序列与之前伪随机序列变化位数的比例。当密钥发生微小改变后，理想位变化率为 50%。在仿真过程中，初始密钥为：0x1F362E5B，0x9ACD5867，0x0C4E4523，0xC6D11B0A，0x4846DE。以此生成长度为10^9 bits 的随机序列，分别改变初始密钥的 1bit，测其位变化率如表 2，其位变化率接近 50%。因此可知，密钥的微小改变引起生成伪随机序列的巨大改变，从而说明本方法生成的随机序列对密钥有高度敏感性。

表 2　伪随机序列的初值敏感性分析表

密钥变化	位变化率
0x1F362E5B-->0x1E362E5B	50.0007%
0x9ACD5867-->0x9ACD5866	49.9980%

3.3　NIST 随机性检测

随机数发生器测试标准[18]是美国国家标准和技术研究院（NIST）发行的联邦信息处理标准，简称 FIPS 标准，此套统计测试方法包括 15 个检测项，既适用于加密算法的随机性测试，也适用于随机数发生器的性能测试。

NIST-STS 检测需要提供长度至少 1G bits 的待检验序列，由于 NIST-STS 检验包将序列分为 1000 个长度为 1M bits 的子序列，所以每一种统计检验都会得到 1000 个值，当 $P>\alpha$ 时，认为该种检验通过。而整个检验包的成功通过需要对如下两点作出判断：

a) P 值分布的均匀性。

b)检验包中每一种检验的通过率，即 $P>\alpha$ 的概率。若 P 值落在置信区间:

$$\left[1-\alpha-3\sqrt{\frac{\alpha(1-\alpha)}{n}},1-\alpha+3\sqrt{\frac{\alpha(1-\alpha)}{n}}\right]$$

则表明序列通过该项测试。（*表示该项包含多个子项）。

用 NIST 随机性测试方法对本方法生成的 1000 组 1 Mbit 数据进行检测，得到的测试结果如表 3 所示。

表 3 NIST SP800-22 测试结果表

测试项目	P-value	proportion	测试结果
Frequence	0.872425	0.996	Pass
Block Frequence	0.392456	0.991	Pass
Cumulative Sums*	0.877083	0.997	Pass
Runs	0.316052	0.984	Pass
Longest Run	0.134172	0.995	Pass
Rank	0.639202	0.987	Pass
FFT	0.371941	0.994	Pass
Overlapping Template	0.135720	0.990	Pass
Universal	0.976878	0.984	Pass
Linear Complexity	0.984415	0.985	Pass
Approximate Entropy	0.385543	0.990	Pass
Serial*	0.848027	0.991	Pass
NonOverlapping Template*	0.999887	0.989	Pass
Random Excursions*	0.889743	0.979	Pass
Random Excursions Variant*	0.877436	0.990	Pass

3.4　信息熵分析

图 3 中，（a）是标准 8bit 灰度图 Lena,用作明文图像进行实验，（b）是将上述方法生成的随机数直接与明文像素值进行异或后生成的密文图像，（c）是原图像的直方图，（d）是加密后图像的直方图。从直方图可以看出，加密后图像的直方图十分均匀，说明原图像的统计规律已经破坏，攻击者很难对原始图像进行恢复。

图像的熵描述图像的平均信息量。熵值越大，图像的随机性越强，其定义如下。

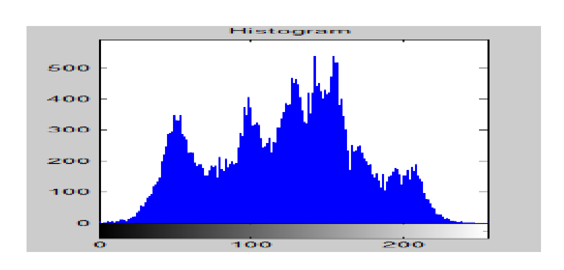
$$H(s)=-\sum_{i=0}^{2^N-1}P(s_i)\log_2 P(s_i)$$

其中：s_i 是信源发出的 2^N 种不同状态，N 是每种状态 s_i 的比特数，$P(s_i)$ 表示状态 s_i 出现的概率。

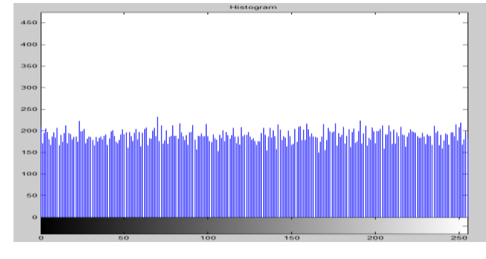
8 bit 灰度图作为信源，可发出 2^8 种不同状态，且每种状态的概率相同，带入熵定义式，8bit 灰度图的理想熵值为 8。因此，本方案生成的随机数用于图像加密后，其熵接近 8，则表明该图像具有良好的随机性。



(a) Lena 图　　(b) Lena 加密图



(c) Lena 直方图



(d) Lena 加密直方图

图 3 Lena 图

与文献[19,20]的信息熵进行比较，结果如表 4。本文生成的随机数用于图像加密后的信息熵接近 8，高于文献[19,20]的信息熵。

表 4 信息熵分析表

方法	信息熵
文献[19]	7.9890
文献[20]	7.9915
本文方法	7.9954

3.5 相关性分析

明文图像位置相邻的像素具有很强的相关性。敌手可利用图像像素在水平、垂直和斜对角方向的规律，对其进行攻击。因此加密后图像相邻位置像素应具有较低的相关性，才能保证图像的安全。相关系数 r_{xy} 衡量加密图像像素的相关性，相关系数接近 0，表明图像像素的相关性低。相关系数定义如下：

$$r_{xy}=\frac{\mathrm{cov}(x,y)}{\sqrt{D(x)}\sqrt{D(y)}}$$

$$E(x)=\frac{1}{\eta}\sum_{i=1}^{\eta}x_i$$

$$D(x)=\frac{1}{\eta}\sum_{i=1}^{\eta}(x_i-E(x))^2$$

$$\mathrm{cov}(x,y)=\frac{1}{\eta}\sum_{i=1}^{\eta}(x_i-E(x))(y_i-E(y))$$

其中，x 和 y 是两个相邻像素的灰度值，η 是选取像素的个数。选取 2000 组像素与文献[5][19]进行水平、垂直和斜对角方向相邻像素进行相关性分析，其结果如表 5（—表示未实现）。本方案生成的随机数用于图像加密相邻像素的相关系数比文献[5]更接近 0，表明图像像素的规律已破坏，相关性降低。

表 5 相关性分析表

相关性分析	水平	垂直	对角
文献[5]	0.0252	-0.0280	0.0176
文献[19]	-0.004	0.001	—
本文方法	-0.008	0.0250	-0.002

3.6 差分攻击

差分攻击通过分析明文差相对应的密文差从而获取相关图像的信息。像素改变率用来衡量图像加密算法抵抗差分攻击的能力。像素改变率越高，表明算法抵抗差分攻击的能力越强。像素改变率定义如下：

$$NPCR=\frac{\sum_{i,j}\delta_a(i,j)}{v}*100\%$$

$$\delta_a(i,j)=\begin{cases}0 & \mathrm{if} C_1(i,j)=C_2(i,j)\\1 & \mathrm{if} C_1(i,j)\neq C_2(i,j)\end{cases}$$

其中，v 是图像像素的总数，C_1 和 C_2 分别为加密图像。

与文献[5,6,19]像素改变率进行比较，结果如表 6。本方案的像素改变率为 99.6%，表明本方案可完全抵抗差分攻击。

表 6 差分分析表

文献	像素改变率
文献[5]	99%
文献[6]	99.5%
文献[19]	99.6%
本文方法	99.6%

本文生成随机数的方法密钥空间高于文献[6]。生成随机数用于图像加密，图像像素的信息熵高于文献[19][20]，相关性低于文献[5]，像素改变率高于文献[5][6]。综合比较分析，本方法生成的随机数具有良好的随机性，可用于图像加密等安全领域。

4 结束语

本文设计了一种新的基于 Logistic 映射生成伪随机数的方法，该方法通过随机选择扰动源交替扰动动态分组的方法，改善了混沌退化对伪随机数发生器安全性的影响，减少重复序列的出现。对其性能进行仿真分析，表明本方法生成的伪随机序列具有良好的密钥敏感性，并且能通过 NIST 随机性检测，从而具有良好的统计特性。

参考文献：

[1] Lorenz E N. Deterministic nonperiodic flow [J]. Journal of the atmospheric sciences, 1963, 20 (2): 130-141.

[2] Wang Xingyuan, Xu Bing, Zhang Huaguang. A multiary number communication system based on hyperchaotic system of 6th-order cellular neural network [J]. Communications in Nonlinear Science and Numerical Simulation, 2010, 15 (1): 124-133.

[3] Mishra M, Mankar V H. Text encryption algorithms based on pseudo random number generator [J]. International Journal of Computer Applications, 2015, 111 (2): 1-6.

[4] Wang Yong, Liu Zhaolong, Ma Jianbin, *et al.* A pseudorandom number generator based on piecewise logistic map [J]. Nonlinear Dynamics, 2016,

83 (4): 2373-2391.

[5] García-Martínez M, Campos-Cantón E. Pseudo-random bit generator based on multi-modal maps [J]. Nonlinear Dynamics, 2015, 82 (4): 2119-2131.

[6] Murillo-Escobar M A, Cruz-Hernández C, Cardoza-Avendaño L, *et al.* A novel pseudorandom number generator based on pseudorandomly enhanced logistic map [J]. Nonlinear Dynamics, 2017, 87 (1): 407-425.

[7] Patidar V, Sud K K, Pareek N K. A pseudo random bit generator based on chaotic logistic map and its statistical testing [J]. Informatica, 2009, 33 (4): 441-452.

[8] François M, Defour D, Negre C. A fast chaos-based pseudo-random bit generator using binary64 floating-point arithmetic [J]. Informatica, 2014, 38 (2): 115-124.

[9] François M, Grosges T, Barchiesi D, *et al.* Pseudo-random number generator based on mixing of three chaotic maps [J]. Communications in Nonlinear Science & Numerical Simulation, 2014, 19 (4): 887-895.

[10] Tamilselvi R, Ravindran G. Image encryption using pseudo random bit generator based on logistic maps with radon transform [J]. Indian Journal of Science and Technology, 2015, 8 (11): 439-46.

[11] Liu Ye, Wang Jun, Fan Jinghui, *et al.* Image encryption algorithm based on chaotic system and dynamic S-boxes composed of DNA sequences [J]. Multimedia Tools and Applications, 2016, 75 (8): 4363-4382.

[12] 董丽华，药国莉. 基于细胞神经网络的伪随机数生成方法 [J]. 通信学报, 2017, 37 (Z1): 85-91. (Dong Lihua, Yao Guoli. Method for generating pseudo random numbers based on cellular neural network [J]. Journal on Communications, 2017, 37 (Z1): 85-91.)

[13] Bahi J M, Fang X, Guyeux C. An optimization technique on pseudorandom generators based on chaotic iterations [J]. arXiv preprint arXiv: 2017: 1706. 08773.

[14] Wang Kaiyu, Yan Qingxin, Yu Shihua, *et al.* High throughput pseudorandom number generator based on variableargument unified hyperchaos [J]. VLSI Design, 2014, 2014: 9.

[15] Selent D. Advanced encryption standard [J]. Rivier Academic Journal, 2010, 6 (2): 1-14.

[16] Wang Bin, Wei Xiaopeng, Zhang Qiang. Cryptanalysis of an image cryptosystem based on logistic map [J]. Optik: International Journal for Light and ElectronOptics, 2013, 124 (14): 1773-1776.

[17] 张雪锋，范九伦. 基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法 [J]. 物理学报, 2010, 59 (4): 2289-2297. (Zhang Xuefeng, Fan Jiulun. Pseudo-random sequence generating method based on LFSR and chaotic system [J]. Acta Physica Sinica, 2010, 59 (4): 2289-2297.)

[18] Rukhin A, Soto J, Nechvatal J, *et al.* A statistical test

[19] suite for random and pseudorandom number generators forcryptographic applications [R]. Booz-Allen and Hamilton Inc Mclean Va, 2001.

[20] Hossain M B, Rahman M T, Rahman A B M S, *et al.* A new approach of image encryption using 3D chaotic map to enhance security of multimedia component [C]// Proc of International Conference on Informatics, Electronics&Vision. 2014: 1-6.

[21] Zahmoul R, Zaied M. Toward new family beta maps for chaotic image encryption [C]// Proc of IEEE InternationalConference on Systems, Man, and Cybernet. 2016: 004052-004057.